

Remotely prepared entanglement: a quantum web page

Todd A. Brun*

Institute for Advanced Study, Einstein Drive, Princeton, NJ 08540

5 July 2001

Abstract

In quantum teleportation, an unknown quantum state is transmitted from one party to another using only local operations and classical communication, at the cost of shared entanglement. Is it possible similarly, using an N party entangled state, to have the state retrievable by *any* of the $N - 1$ possible receivers? If the receivers cooperate, and share a suitable state, this can be done reliably. The N party GHZ is one such state; I derive a large class of such states, and show that they are in general not equivalent to the GHZ. I also briefly discuss the problem where the parties do not cooperate, and the relationship to multipartite entanglement quantification. I define a new set of entanglement monotones, the entanglements of preparation.

Key Words: Quantum information, quantum algorithms, teleportation, entanglement measures, multipartite entanglement.

1 Introduction

Much of the recent progress in quantum information theory has stemmed from the idea of using quantum entanglement as a resource for carrying out operations on quantum states. In particular, shared entanglement between two parties can be used to *teleport* an unknown quantum state using only local operations (measurements and unitary transformations) and classical communication (LOCC) [1]; it can also enable two classical bits to be transmitted by a single quantum bit (*q-bit*) via *superdense coding* [2].

*Email: tbrun@ias.edu. Phone: (609) 734-8335. FAX: (609) 951-4489.

The accepted unit of quantum entanglement (at least for pure states) is the maximally-entangled (EPR) pair, or *e-bit*. Any such pair is equivalent under local unitary transformations to the state

$$|\Psi_{AB}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}. \quad (1)$$

The entanglement of any bipartite pure state can be measured in e-bits, and in the asymptotic limit (i.e., where the two parties have many copies of a state) any two states with the same entanglement can be reversibly interconverted [3].

By contrast, the case with more than two parties is far from clear. No single number suffices to describe the entanglement of multipartite states, even asymptotically; nor is it known how many numbers are needed, or even if the number is finite; nor are general algorithms known for reversibly interconverting states [4]. In the face of these limits, it seems reasonable both to try to generalize bipartite results to multipartite systems, and to relate multipartite entanglement to the bipartite measure.

2 The quantum web page

Let us briefly review the teleportation protocol between two parties, usually known as Alice and Bob. It is assumed that they share a maximally entangled pair of q-bits (one e-bit). In addition, Alice has another q-bit in an unknown state $|\chi\rangle$. She jointly measures this q-bit together with her half of the entangled pair in the Bell basis,

$$|\phi^\pm\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}, \quad |\psi^\pm\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}, \quad (2)$$

and transmits the result of her measurement (2 classical bits) to Bob. This measurement of course destroys Alice's copy of the state she wishes to send. By performing one of four unitary transformations on his half of the entangled pair, Bob can reconstruct the state $|\chi\rangle$ [1].

The problem I consider is a simple generalization of teleportation to N parties. Suppose that these N parties (Alice, Bob, Cara, David... , Nancy) share an N q-bit pure state. One of them, say Alice, is given another q-bit in an unknown state. She wishes to combine this state with the shared state in such a way that any of the other $N - 1$ parties can retrieve it using only LOCC. If we make an analogy between ordinary teleportation and an email, this procedure would be more like a *quantum web page*: making a state available to anyone in a given network.

Suppose that one party, say Bob, decides to retrieve the state. He clearly will only be able to do so with the cooperation of the other $N - 2$ parties. If these parties do not assist, he will at best share an entangled mixed state with Alice, which is insufficient for reliable teleportation to be carried out. An easy way to see this is to note that if Bob could retrieve the state without the assistance of the others, so could Cara or any other party; and the state would have been copied, which is forbidden by the no-cloning theorem [5].

If the other parties cooperate the procedure can indeed be carried out. Suppose that they share an N party GHZ state,

$$|\Psi_{A\dots N}\rangle = (|0\dots 0\rangle + |1\dots 1\rangle)/\sqrt{2}. \quad (3)$$

These states are often considered to be *maximally entangled*, though in the absence of a measure of multipartite entanglement it is not clear that this makes sense [6]. Let the parties $C\dots N$ measure their q-bits in the basis

$$|0'\rangle = (|0\rangle - |1\rangle)/\sqrt{2}, \quad |1'\rangle = (|0\rangle + |1\rangle)/\sqrt{2}. \quad (4)$$

After the first party measures his or her q-bit, the remaining $N - 1$ parties will share an $N - 1$ party GHZ state. This becomes an $N - 2$ party GHZ with the next measurement, and so on, until Alice and Bob are left with the state

$$|\Psi_{AB}\rangle = (|00\rangle + (-1)^{p(s)}|11\rangle)/\sqrt{2}, \quad (5)$$

where s denotes the sequence of $N - 2$ measurement results, and $p(s)$ is the parity of the sequence s . This is a maximally entangled pair, and can be used to teleport the unknown state from Alice to Bob.

Since the order in which these operations are performed doesn't matter, Alice can carry out her part of the teleportation protocol before any of the other measurements are carried out, even before it has been decided which of the $N - 1$ parties will retrieve the state. She jointly measures in the Bell basis the q-bit whose state she wishes to make available, together with her part of the N bit state, and broadcasts the measurement result to the other parties. At that point, any of them can retrieve the state with the cooperation of the others, with no further action on the part of Alice; indeed, Alice no longer shares entanglement with the other parties.

We have seen how this can be done using an N party GHZ state, but is this the only state which will work? Any state which allows a maximally-entangled pair to be prepared between Alice and any other party, using only LOCC, could be used instead. I will call all such states *web states*, and call

the basis in which each party measures his or her bit the *preparation basis*. For now, I restrict myself to the case where the choice of this basis does not depend on which two parties are to share the pair, nor on the outcome of measurements by other parties. I will call this case *context-free*.

If we rewrite the GHZ in terms of the preparation bases of all the parties, it takes the form

$$|\Psi_{A\dots N}\rangle = \frac{1}{\sqrt{2^{N-1}}} \sum_{\text{even } s} |s\rangle, \quad (6)$$

where s is a sequence of N 0's and 1's, and the sum is restricted only to those with an even number of 1's. In this form it is easy to see that any measurement of $N - 2$ of the bits in their preparation bases will leave the other two in a maximally-entangled state.

Are all such context-free web states equivalent to the N party GHZ? No, they are not. Consider the following state:

$$|\Psi_{A\dots N}\rangle = \frac{1}{\sqrt{2^{N-1}}} \sum_{\text{even } s} \exp(i\theta(s)) |s\rangle, \quad (7)$$

where the $\theta(s)$ are 2^{N-1} arbitrary phases. Just as with the GHZ, measuring any $N - 2$ of the bits in this basis will leave the other two in a maximally entangled state, so this state can be used for a quantum web page. But a state of this form cannot, in general, be transformed into a GHZ by LOCC. There are 2^{N-1} phases; at most $N + 1$ of these can be eliminated by local unitary transformations. Thus, such states can only be transformed into the GHZ in general for $N = 3$.

In the next section, I will prove that all web states with context-free preparation bases are equivalent to a state of the form (7) under local unitary transformations. I will also prove that if a state allows a maximally entangled pair to be prepared between one particular party (say Alice) and any of the others, then it allows a maximally entangled pair to be prepared between *any* two parties, and hence can be put in the form (7).

3 N q-bit web states

Suppose we select two parties (Alice and Bob) for whom we wish to prepare an EPR pair. The other $N - 2$ parties measure their bits in the correct preparation basis, producing a measurement results s (where s denotes a sequence of $N - 2$ 0's and 1's). For any outcome s , Alice and Bob must be

left with a state $|\Psi_{AB}(s)\rangle$ which is maximally entangled. So the full state can be written

$$|\Psi_{A\dots N}\rangle = \sum_s c_s |\Psi_{AB}(s)\rangle \otimes |s\rangle, \quad (8)$$

where the c_s are real, positive coefficients with normalization

$$\sum_s c_s^2 = 1. \quad (9)$$

The most general form of a maximally entangled pair is

$$\begin{aligned} |\Psi_{AB}\rangle &= \cos \alpha \left(e^{i\theta} |00\rangle + e^{i\phi} |11\rangle \right) / \sqrt{2} \\ &\quad + \sin \alpha \left(e^{i\omega} |01\rangle - e^{i(\theta+\phi-\omega)} |10\rangle \right) / \sqrt{2}, \end{aligned} \quad (10)$$

where $0 \leq \alpha \leq \pi/2$ and θ, ϕ, ω are arbitrary phases. One can derive this form straightforwardly, by writing down an arbitrary two-bit pure state and imposing the restriction that $\text{Tr}_B\{|\Psi_{AB}\rangle\langle\Psi_{AB}|\} = \hat{1}/2$; this lets one eliminate three degrees of freedom, yielding (10). We assume without loss of generality that q-bit B is also written in its preparation basis. We can now write the state (8) in the form

$$\begin{aligned} |\Psi_{A\dots N}\rangle &= \frac{1}{\sqrt{2}} \sum_s c_s \left[\cos \alpha_s \left(e^{i\theta_s} |00\rangle + e^{i\phi_s} |11\rangle \right) \right. \\ &\quad \left. + \sin \alpha_s \left(e^{i\omega_s} |01\rangle - e^{i(\theta_s+\phi_s-\omega_s)} |10\rangle \right) \right] \otimes |s\rangle. \end{aligned} \quad (11)$$

For this to be a web state, we must be able to exchange Bob's q-bit with that of any other party and recover a state of form (11). Suppose we wish to exchange Bob's bit with that of the M th party. Let us group all sequences s into pairs (s_0, s_1) which are identical except at the M th bit, which is 0 for s_0 and 1 for s_1 . If we exchange Bob's q-bit with the M th q-bit, the state becomes

$$\begin{aligned} |\Psi_{A\dots N}\rangle &= \frac{1}{\sqrt{2}} \sum_{(s_0, s_1)} \left[(c_{s_0} \cos \alpha_{s_0} e^{i\theta_{s_0}} |00\rangle - c_{s_0} \sin \alpha_{s_0} e^{i(\theta_{s_0}+\phi_{s_0}-\omega_{s_0})} |10\rangle \right. \\ &\quad + c_{s_1} \cos \alpha_{s_1} e^{i\theta_{s_1}} |01\rangle - c_{s_1} \sin \alpha_{s_1} e^{i(\theta_{s_1}+\phi_{s_1}-\omega_{s_1})} |11\rangle) \otimes |s_0\rangle \\ &\quad + (c_{s_0} \cos \alpha_{s_0} e^{i\phi_{s_0}} |10\rangle + c_{s_0} \sin \alpha_{s_0} e^{i\omega_{s_0}} |00\rangle \\ &\quad \left. + c_{s_1} \cos \alpha_{s_1} e^{i\phi_{s_1}} |11\rangle + c_{s_1} \sin \alpha_{s_1} e^{i\omega_{s_1}} |01\rangle) \otimes |s_1\rangle \right]. \end{aligned} \quad (12)$$

For this to be a web state, there must be new parameters $c'_s, \alpha'_s, \theta'_s, \phi'_s, \omega'_s$ which put (12) in form (11).

Comparing (12) and (11) term by term, we immediately see that we must have

$$\begin{aligned} c'_{s_0} \cos \alpha'_{s_0} &= c_{s_0} \cos \alpha_{s_0} = c_{s_1} \sin \alpha_{s_1} , \\ c'_{s_0} \sin \alpha'_{s_0} &= c_{s_0} \sin \alpha_{s_0} = c_{s_1} \cos \alpha_{s_1} , \\ c'_{s_1} \cos \alpha'_{s_1} &= c_{s_0} \sin \alpha_{s_0} = c_{s_1} \cos \alpha_{s_1} , \\ c'_{s_1} \sin \alpha'_{s_1} &= c_{s_0} \cos \alpha_{s_0} = c_{s_1} \sin \alpha_{s_1} . \end{aligned} \quad (13)$$

This must hold for every pair (s_0, s_1) , and for every choice of M , which implies that

$$c_s = 1/\sqrt{2^{N-2}} \quad \forall s , \quad (14)$$

and that

$$\alpha_s = \alpha_{p(s)} \quad \forall s , \quad \alpha_1 = \pi/2 - \alpha_0 , \quad (15)$$

where $p(s)$ is the parity of the string s , with $p(s) = 0$ for even strings, $p(s) = 1$ for odd strings. This just means that $\cos \alpha_0 = \sin \alpha_1$ and $\sin \alpha_0 = \cos \alpha_1$.

In a similar way we can examine the phases of (12). It is only possible to preserve the form of (11) if

$$\exp i(\phi_{s_1} - \omega_{s_1}) = -\exp i(\phi_{s_0} - \omega_{s_0}) . \quad (16)$$

Again, this must hold for any pair (s_0, s_1) , and for any choice of M , which gives us the requirement

$$\omega_s = \phi_s + \gamma + p(s)\pi , \quad (17)$$

where γ is a constant phase, and $p(s)$ is once again the parity of the string s . We can eliminate the phase γ by a local unitary transformation

$$\begin{aligned} |0\rangle_A &\rightarrow |0\rangle_A , & |0\rangle_B &\rightarrow |0\rangle_B , \\ |1\rangle_A &\rightarrow e^{i\gamma}|1\rangle_A , & |1\rangle_B &\rightarrow e^{-i\gamma}|1\rangle_B , \end{aligned} \quad (18)$$

which leaves the physical preparation basis of B unchanged.

With these restrictions, we now see that any context-free web state can be written in the form

$$\begin{aligned} |\Psi_{A\dots N}\rangle &= \frac{1}{\sqrt{2^{N-1}}} \sum_s \left[\cos \alpha_{p(s)} \left(e^{i\theta_s} |00\rangle + e^{i\phi_s} |11\rangle \right) \right. \\ &\quad \left. + (-1)^{p(s)} \sin \alpha_{p(s)} \left(e^{i\phi_s} |01\rangle - e^{i\theta_s} |10\rangle \right) \right] \otimes |s\rangle . \end{aligned} \quad (19)$$

But is this the simplest form possible? Let us perform a local unitary transformation on q-bit A:

$$\begin{aligned} |0\rangle_A &\rightarrow \cos \alpha_0 |0\rangle_A + \sin \alpha_0 |1\rangle_A, \\ |1\rangle_A &\rightarrow -\sin \alpha_0 |0\rangle_A + \cos \alpha_0 |1\rangle_A. \end{aligned} \quad (20)$$

This must still be a web state, since a local unitary on A will leave any maximally entangled pair still maximally entangled. We can easily check that the state (19) now takes the form

$$|\Psi_{A\dots N}\rangle = \frac{1}{\sqrt{2^{N-1}}} \sum_s \left\{ \begin{array}{l} \exp(i\theta(s))|00\rangle + \exp(i\phi(s))|11\rangle \\ \exp(i\theta(s))|10\rangle - \exp(i\phi(s))|01\rangle \end{array} \right\} \otimes |s\rangle, \quad (21)$$

where the upper (lower) line is used for even (odd) strings s . This expression is exactly equivalent to the form (7) given in section 2. So we see that *any* context-free web state can be put in form (7), and any state which allows context-free preparation of an EPR between one party and any of the others must allow preparation of an EPR between *any* two parties.

4 Generalizations

4.1 Contextual web states

The most obvious generalization we might consider is to states which are not context-free, i.e., where the choice of measurement basis depends on which two parties are to have an EPR pair prepared. Logically this should be a much larger class of states than that of context-free web states.

I have not derived a general prescription for all contextual web states, but some obvious general characteristics suggest themselves. Any web state must give a reduced density matrix proportional to the identity for all q-bits:

$$\text{Tr}_{N-1} \{ |\Psi_{A\dots N}\rangle \langle \Psi_{A\dots N}| \} = \rho = \hat{1}/2. \quad (22)$$

Also, any *pair* of q-bits A and M must have a reduced density matrix ρ_{AM} with entanglement of assistance (or hidden entanglement) equal to 1 [7, 8]. These are necessary but probably not sufficient conditions. For $N = 3$, these requirements are enough to prove that *all* web states are equivalent to the GHZ under local unitary transformations, and hence are context-free.

For $N = 4$ we can find examples which are not equivalent to context-free states, and hence cannot be written in the form (7). For instance, the state

$$|\Psi_{ABCD}\rangle = \frac{1}{2} \left[(|00\rangle + |11\rangle) \otimes |00\rangle + (|00\rangle - |11\rangle) \otimes |11\rangle \right], \quad (23)$$

allows an EPR to be prepared between A and B or between C and D by measuring the other two bits in the given basis. However, by measuring in that basis it is impossible to prepare an EPR between any other pair.

We could instead measure two bits in the basis

$$\begin{aligned} |0'\rangle &= (|0\rangle + |1\rangle) / \sqrt{2}, \\ |1'\rangle &= (|0\rangle - |1\rangle) / \sqrt{2}. \end{aligned} \tag{24}$$

A maximally-entangled state can be prepared between A and C, B and C, A and D or B and D by measuring the other two bits in the basis (24), but *not* between A and B or C and D. This state (23) is thus a web state, but a contextual one.

An even more general possibility would be to allow the measurement bases of some bits to depend on measurement outcomes for others; or to allow general positive-operator valued measurements (POVMs); or both. Characterizing this large class of operations, though, is not easy [9]; no simple form is known for a general LOCC procedure.

4.2 Preparing other states

We might also ask about preparing shared states other than EPR pairs. Because an EPR pair can be reliably transformed into any two q-bit state by LOCC [10], the web states we have considered can also produce any such state between any two parties.

For multipartite states the situation is less clear, but some results follow easily. Note that if one party carries out a measurement on an N party context-free web state in his or her preparation basis, the other $N - 1$ parties are left with an $N - 1$ party context-free web state. For $N = 3$, all such states are equivalent to the 3 party GHZ. So for $N > 3$, any state of form (7) also allows the preparation of a GHZ among any three parties.

For more general cases, a procedure like that of section 3 might be carried out to find all N party states which allow some particular $M < N$ party state to be reliably prepared among any M participants. But there seems no guarantee that the results will in general be as simple as those for the EPR pair.

4.3 The noncooperative problem and cloning

This quantum web page algorithm requires that all the parties cooperate in enabling the selected party (say Bob) to retrieve the state $|\chi\rangle$ that Alice has

made available. Without this cooperation, at best Bob will retrieve a mixed state.

However, we can imagine a version of this problem in which the parties do *not* cooperate, and ask what state should be used to maximize the fidelity of Bob's state ρ_B with the state $|\chi\rangle$ he is attempting to retrieve. Let $|\Psi_{A\dots N}\rangle$ be the shared initial state, and $|\chi\rangle$ be the state that Alice is trying to make available. After Alice carries out her part of the procedure (which is just like her part of the cooperative procedure), the other $N - 1$ parties are left with a new joint state $|\Psi'_{B\dots N}\rangle$. The reduced state of Bob's subsystem is

$$\rho_B = \text{Tr}_{C\dots N} \{ |\Psi'_{B\dots N}\rangle \langle \Psi'_{B\dots N}| \} , \quad (25)$$

and we wish to maximize the fidelity

$$F = \langle \chi | \rho_B | \chi \rangle . \quad (26)$$

This fidelity should be the same for any party and for any state $|\chi\rangle$, so we see that this is the same as $N - 1$ party *symmetric cloning* [11]. The maximum fidelity achievable by symmetric cloning to $N - 1$ q-bits is $F = (2N - 1)/(3(N - 1))$. The class of states which are used in the noncooperative case is quite different from the class of web states; examples which achieve this maximum fidelity have been discovered, e.g., by Dür [12] and Koashi et al. [13]. A related problem has also been considered by Dür and Cirac [14].

Note that one must not confuse the *cloning fidelity* F given by (26) with the *singlet fraction* F_s of the N -partite state. If we trace out parties $C\dots N$ of $|\Psi_{A\dots N}\rangle$ to get the bipartite density matrix ρ_{AB} , the singlet fraction is

$$F_s = \max_{|\Psi_{AB}\rangle} \langle \Psi_{AB} | \rho_{AB} | \Psi_{AB} \rangle , \quad (27)$$

where the maximum is over all *maximally entangled states* $|\Psi_{AB}\rangle$. The maximum of F_s is considerably lower than F , and is bounded by $F_s \leq N/2(N - 1)$. This distinction is brought out in [15].

4.4 Multipartite entanglement

The problem of characterizing multipartite entanglement remains largely unsolved, especially in the asymptotic limit [4]. The idea behind these web states suggests a set of possibly useful quantities that can be calculated from a multipartite pure state.

The *entropy of entanglement* for an entangled pair is

$$\mathcal{E}(|\Psi_{AB}\rangle) = -\text{Tr}_A\{\rho_A \log_2 \rho_A\} , \quad (28)$$

where ρ_A is the reduced density matrix of q-bit A,

$$\rho_A = \text{Tr}_B\{|\Psi_{AB}\rangle\langle\Psi_{AB}|\} . \quad (29)$$

Suppose we perform some LOCC procedure (e.g., a measurement) on an N -partite system which is initially in a pure state $|\Psi_{A\dots N}\rangle$; denote this procedure by O , with outcomes o_i occurring with probability p_i , and assume that it leaves the pair of subsystems A and B in a *pure* state $|\Psi_{AB}(o_i)\rangle$. (That is, there is no entanglement left with C...N.) Then we can define the *average preparation entanglement* of A and B under O :

$$\bar{\mathcal{E}}_{AB}(|\Psi_{A\dots N}\rangle, O) = \sum_i p_i \mathcal{E}(|\Psi_{AB}(o_i)\rangle) . \quad (30)$$

This quantity will vary enormously depending on the choice of O . We can, however, look for the maximum, and use that to define the *entanglement of preparation*

$$\mathcal{E}_{AB}^p(|\Psi_{A\dots N}\rangle) \equiv \max_O \bar{\mathcal{E}}(|\Psi_{A\dots N}\rangle, O) . \quad (31)$$

For an N -partite system, we can define the entanglement of preparation between any two parties. This quantity is similar to the entanglement of assistance (or hidden entanglement) $\mathcal{E}^a(\rho_{AB})$ [7, 8]; however, in general it will be lower, $\mathcal{E}_{AB}^p(|\Psi_{A\dots N}\rangle) \leq \mathcal{E}^a(\rho_{AB})$, since the measurements yielding the entanglement of preparation must respect the division of C...N into local subsystems, while the entanglement of assistance has no such constraint. By definition, any web state must have entanglement of preparation 1 between q-bit A and any other q-bit.

Note that we can relax the restriction on O (to operations which leave A and B in a pure state) by replacing the entropy of entanglement in (30) with the *entanglement of formation* $\mathcal{E}^f(\rho_{AB}(o_i))$ [16]. With this change, the maximum in (31) becomes a maximum over *all* LOCC procedures O . It is not hard to see that the value of $\mathcal{E}_{AB}^p(|\Psi_{A\dots N}\rangle)$ is unchanged by this alteration; the maximum will always be achieved by an operation O which *does* leave A and B in a pure state, for which the entropy of entanglement and the entanglement of formation give equal values.

An important point is that, by construction, $\mathcal{E}_{AB}^p(|\Psi_{A\dots N}\rangle)$ is an *entanglement monotone*. That is, the value of \mathcal{E}_{AB}^p cannot increase on average if

one performs some LOCC procedure on the state $|\psi_{A\dots N}\rangle$. Clearly, if it *could* increase, then the operation O would not be the maximum. Such monotones are important in trying to understand the entanglement properties of multipartite states. In a similar way, any numerical function of the state can be used to define an entanglement monotone; one simply takes the average value of the function under the action of some LOCC procedure O , and maximizes over all O . Of course, $\mathcal{E}_{AB}^p(|\Psi_{A\dots N}\rangle)$ may be difficult to calculate exactly for a general state; however, one may still be able to derive useful bounds on it.

Finally, the entanglement of preparation is a *superadditive* quantity. Suppose that the parties $A\dots N$ share *two* systems with N subsystems each, the two systems being in pure states $|\Psi_{A\dots N}\rangle$ and $|\Phi_{A\dots N}\rangle$, respectively. We can consider these jointly as a single N -partite system in state $|\Psi_{A\dots N}\rangle \otimes |\Phi_{A\dots N}\rangle$. Then the entanglement of preparation for this joint state must satisfy

$$\mathcal{E}_{AB}^p(|\Psi_{A\dots N}\rangle \otimes |\Phi_{A\dots N}\rangle) \geq \mathcal{E}_{AB}^p(|\Psi_{A\dots N}\rangle) + \mathcal{E}_{AB}^p(|\Phi_{A\dots N}\rangle). \quad (32)$$

This is similar to the class of entanglement monotones derived in [17].

5 Conclusions

It is possible to produce a quantum analogue of a web page: a procedure by which a quantum state is made available by one party to any of a group of others, using only a shared initial state, local operations and classical communication. Unlike the classical case, however, retrieving the quantum state requires cooperation among the $N - 1$ possible recipients, and only one can actually retrieve it.

I have presented a large class of N q-bit pure states which can be used for the quantum web page, of which the N party GHZ is an example, and argued that an even larger class is potentially available. This problem suggests a set of quantities, the *entanglements of preparation* of the various pairs, which may prove useful in the ongoing attempt to characterize multipartite entanglement, especially since these quantities are entanglement monotones. This problem could be generalized in many ways; but for the present, these related problems remain unsolved.

Acknowledgments

I would like to thank Oliver Cohen and Bob Griffiths for their feedback on this problem, and for looking over the manuscript; and Michele Mosca and Alain Tapp for inviting my contribution to this special issue of *Algorithmica*.

After this work was completed I became aware of a paper by Briegel and Raussendorf [18], which includes a definition of *maximal connectedness* which is the same as my web page property; they also give a particular set of states which have that property. In particular, their state $|\phi_4\rangle$ is equivalent to the contextual web state (23) in this paper.

This work was supported by DOE Grant No. DE-FG02-90ER40542.

References

- [1] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
- [2] C.H. Bennett and S. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
- [3] C.H. Bennett, H.J. Bernstein, S. Popescu and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
- [4] C.H. Bennett, S. Popescu, D. Rohrlich, J.A. Smolin, A.V. Thapliyal, to appear in Phys. Rev. A, quant-ph/9908073.
- [5] W.K. Wootters and W.H. Zurek, Nature **299**, 802 (1982).
- [6] A. Higuchi and A. Sudbery, Phys. Lett. A **273**, 213, (2000).
- [7] O. Cohen, Phys. Rev. Lett. **80**, 2493 (1998).
- [8] D.P. DiVincenzo, C.A. Fuchs, H. Mabuchi, J.A. Smolin, A.V. Thapliyal, A. Uhlmann, quant-ph/9803033.
- [9] C.H. Bennett, D.P. DiVincenzo, C.A. Fuchs, T. Mor, E. Rains, P.W. Shor, J.A. Smolin, W.K. Wootters, quant-ph/9804053.
- [10] M.A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).
- [11] V. Bužek, S. Braunstein, M. Hillery and D. Bruß, Phys. Rev. A **56**, 3446 (1997); V. Bužek, M. Hillery, quant-ph/9801009.
- [12] W. Dür, Phys. Rev. A **63**, 020303(R) (2001).

- [13] M. Koashi, V. Buzek and N. Imoto, quant-ph/0007086.
- [14] W. Dür and J.I. Cirac, J. Mod. Optics **47**, 247 (2000).
- [15] M. Horodecki, P. Horodecki and R. Horodecki, quant-ph/9807091.
- [16] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin and W.K. Wootters, Phys. Rev. A **54**, 3824 (1996).
- [17] H. Barnum and N. Linden, quant-ph/0103155.
- [18] H.J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).